



# CVE-2021-33394

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-33394
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-05-27 19:15:00 UTC
<b>Updated</b>	2021-06-02 17:31:00 UTC
<b>Description</b>	Cubecart 6.4.2 allows Session Fixation. The application does not generate a new session cookie after the user is logged in.

## Risk And Classification

**Problem Types:** CWE-384

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Cubecart</a>	<a href="#">Cubecart</a>	6.4.2	All	All	All

## References

Reference	Source	Link	Tags
#2870 - session fixation · cubecart/v6@aac7b3a · GitHub	CONFIRM	<a href="#">github.com</a>	
POC/Session Fixation in Cubecart 6.4.2.md at main · xoffense/POC · GitHub	MISC	<a href="#">github.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)